Review and Confirm Your Submission

Your incident report has NOT yet been submitted. Please review and confirm your submission below.

To submit your report, please review the information below to verify the accuracy of the report and click the SUBMIT button. Or if you would like to revise your incident report you may click the EDIT buttons to return to the previous page.

Contact Information

Edit

Required fields are marked with an asterisk (*).

I am: *

- (●) The impacted user
- ( ) Reporting on behalf of the impacted user

Your Contact Information

First Name: John

Last Name: Fouts

Telephone

5029560052

Email *

icreateupwardspirals@gmail.com

Organization Details

Edit

Required fields are marked with an asterisk (*).

The Impacted Organization's Details

What type of organization are you reporting for?*

I am an individual, not an organization

Please enter the impacted organization's internal tracking number (if applicable):

N/A

Incident Description

Edit

Required fields are marked with an asterisk (*).

Incident Description

When approximately, did the incident start? *

07 / 01 / 2024 , 12 : 00 AM

When was this incident detected? *

05 / 25 / 2025 , 12 : 00 AM

Please enter a brief description of the incident *

A new Apple iPhone 15+ purchased in Summer 2024 from T-Mobile (Louisville, KY) exhibited consistent signs of firmware- and baseband-level compromise across both iOS 17 and iOS 18.

Key indicators include:

Impact Details

Edit

Required fields are marked with an asterisk (*).

Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised? *

Additional questions may apply

- (●) Yes
- ( ) No

System Impact

Please define the functional impact to the organization by selecting one of the following *

Significant Impact to Critical Services

What is the number of systems impacted? *

1

How many users are impacted? *

2

How was this incident detected?

- [ ] Administrator
- [ ] User
- [ ] Anti-Virus (AV) Software
- [x] Other
- [ ] Intrusion Detection System (IDS)
- [ ] Unknown
- [ ] Log Review

Please enter details *

Detected through first-hand observation of abnormal device behavior, confirmed via iOS Privacy settings and Apple analytics logs. Microphone activations occurred with no authorized app usage or permissions granted. Siri activated without user input. Repeated call routing anomalies were observed during attempts to contact public federal numbers. Device

What operating systems (OS) are impacted?

Operating System #1

Operating System name: iOS

Operating System Version: 17.x

Remove OS

Operating System #2

Operating System name: iOS

Operating System Version: 18.x

Remove OS

+ Add Detail For Impacted OS

What is the function of the system(s) affected? Please select all that apply *

- [ ] Application Server(s)
- [ ] Switch(es)
- [ ] Database Server(s)
- [ ] Time Server(s)
- [ ] Desktop(s)
- [ ] Web Server(s)
- [x] Domain Name Server(s)
- [x] Laptop(s)
- [ ] Firewall(s)
- [x] Other Server(s)
- [ ] ICS/SCADA System(s)
- [ ] Mail Server(s)
- [x] Router(s)

Please Enter the Indicator Type

Indicator Type #1

Please Enter the Indicator Type

Network - Domain Name(s)

Indicators

eap01.t-mobile.com

gdmf.apple.com

captive.apple.com

Indicator Context

These domains were observed in connection with unusual or unauthorized traffic patterns. eap01.t-mobile.com and gdmf.apple.com appeared during device provisioning and network reattachment events, even when SIM was not present. captive.apple.com was invoked under anomalous conditions

Remove Indicator

Indicator Type #2

Please Enter the Indicator Type

Network - IPv4 Address(es)

Indicators

Additional information available upon request.

Indicator Context

Call attempts to the White House (and other federal offices) were consistently intercepted or misrouted, despite SIM card removal. The device used internal routing (likely baseband firmware or eSIM override) to maintain call paths. DNS resolution and packet flow were inconsistent with typical iOS behavior, pointing to a firmware-

Remove Indicator

Indicator Type #3

Please Enter the Indicator Type

Network - URL

Indicators

https://gdmf.apple.com/v2/assets/config/...

https://init.itunes.apple.com/...

https://captive.apple.com/hotspot-detect.html

Indicator Context

These URLs are part of Apple's official traffic flow but were repeatedly triggered in circumstances suggesting non-standard usage — including during OS idle states, airplane mode, or while all app permissions were revoked. They correlate with periods of suspicious background traffic and observed device mic activation.

Remove Indicator

Indicator Type #4

Please Enter the Indicator Type

Network - Network Traffic

Indicators

Encrypted outbound traffic during sleep mode and with no apps open

Device re-established network sessions without user initiation

Indicator Context

Traffic patterns indicated baseband or firmware bypass of user configuration. This included persistent DNS activity when device was nominally offline, and rerouting of sensitive calls even under factory-reset and non-carrier conditions. Patterns mirror behavior seen in advanced persistent threat (APT) environments.

Remove Indicator

Indicator Type #5

Please Enter the Indicator Type

Network - Autonomous System(s) (AS)

Indicators

/private/var/db/analyticsd/

/private/var/logs/AWDD/

/usr/share/zoneinfo/

Indicator Context

These directories logged unauthorized system events, including microphone activation while all app-level permissions were denied. Manual review confirmed microphone activation from unknown internal triggers with no apps in foreground. Logs persisted across reboots and device resets. Apple analytics reports (from within

Remove Indicator

+ Add Indicator Type

Enter a Common Vulnerabilities and Exposure Identifier (CVE-ID).
Please do not include the CVE prefix (e.g., 2014-7654321):

No CVE Match

Observed Activity

Where was the activity observed *

Level 5 - Critical System Manageme

Characterize the observed activity at its most severe level *

Effect/Consequence

Impact Information

What is the known informational impact from the incident? *
Additional questions may apply

Critical Systems Data Breach

Number of records impacted *

5000

Recovery From Incident

Please select the organization's recoverability for this incident *
Additional questions may apply

Not Recoverable

Please provide details here

My phone (Apple iPhone 15+) shows signs of firmware compromise, call interception, and unauthorized baseband behavior — these are indicators of a breach of device security architecture, not just data exposure.

This encompasses the activation of microphones, traffic rerouting, DNS-

Does your agency currently consider this to be a breach that must be reported to Congress within 30 days in accordance with OMB Policy?

- ○ Yes
- ◉ No

Privacy Act Statement

Authority: 5 U.S.C. § 301 and 44 U.S.C. § 3101 authorize the collection of this information.

Purpose: The primary purpose for the collection of this information is to allow the Department of Homeland Security to contact you about your request.

Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.

Disclosure: Some entities are regulatory or statutorily required to submit incident reports to DHS, and those entities must provide information in this form as required by applicable statute, regulation, or similar mandate. Failure for provide this information may result in inaccurate record keeping of the entity's compliance. For non-mandatory incident reporting, providing this information is voluntary. However, failure to provide this information will prevent DHS from contacting you in the event there are questions about your report.

Save and Download Cancel Submit